4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,607	06/01/2001	Christophe Clavier	032326-132	2078

21839 7590 02/15/2005

BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/807,607	CLAVIER ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *04/16/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on June 1, 2001. Claims 1 – 12 were originally received for consideration. Per the received preliminary amendments, claims 13-16 have been added, and claims 11-12 have been cancelled. Claims 1 – 10, and 13-16 are currently being considered.

Information Disclosure Statement

2. An initialed and dated copy of the Applicant's IDS form 1449 has been attached to this Office action.

Specification

3. The disclosure is objected to because of the following informalities: "used" is misspelled on page 22, line 12 of the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. The term "some" in claim 1 is a relative term, which renders the claim indefinite. The term "some" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term "some" should be replaced with a term that better defines the number or nature of the "instructions" that are being described in the limitation. The term "some" has been ignored for purposes of examinations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1 –10, 13-16are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Kocher et al. (U.S. Patent No. 6,278,783).

Regarding claim 1, Leppek discloses:

A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm having a secret key, comprising the following steps:

"***executing some instructions in the algorithm that are critical to said attacks with a first manipulating means to deliver output data on the basis of input data***" (Figure 2, column 4 lines 7-51), wherein at least two different sequences of encryption operators are selected to encrypt the data;

"***executing others of said critical instructions with other manipulating means that are derived from said first manipulating means"*** (Figure 2, column 4 lines 7-51). Leppek does not explicitly disclose that this manipulating means is by "***complementation of at least one of the input data and said output data, so that the output data and the data derived from said output data are unpredictable***." Kocher teaches a method of using DES to minimize information leak using smart cards and other cryptosystems, and discloses the "***complementation of data***" (column 6 lines 29-63, column 9 lines 5-23), where the complements are taken to prevent different sources of information leakage such as "observation of the power consumption and/or timing can reveal whether the carried bit in each round equal zero or one" (column 5 lines 8-15). Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures. Leppek uses a series of encryption operators with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the

possibility that "observation of the power consumption and/or timing can reveal whether the carried bits in each round equal zero or one, revealing some or all of the key bits" (Kocher column 5 lines 7 – 15). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence which prevents the usefulness of an attack which observes the power consumption and/or timing to determine whether the carried bits are zeroes or ones, which reveals the bits of the key.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Leppek discloses:

A countermeasure method according to claim 1, wherein said "***first and other manipulating means are selected for use on the basis of one-half probability statistical relationship***" (column 4 lines 33-52), wherein in the simplest form, there are two different sequences of operators that can be selected randomly equating to a fifty percent probability that either sequence will be chosen.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Leppek discloses a countermeasure method according to claim 2, wherein said "***method comprises executing a first sequence and a second sequence, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship***" (Figure 2, column 4 lines 7-52), wherein there are

two different sequence of operators that can be selected randomly. Leppek does not explicitly disclose any particular encryption algorithm but states that they "need not be any particular type of encryption algorithm" (column 4 lines 10-17). Kocher discloses the use of a modified DES encryption algorithm which consists of sixteen rounds (Figure 1), which can then incorporated in the different sequences of Leppek to produce an encrypted stream. Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures. Leppek uses a series of encryption operators with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the possibility that "observation of the power consumption and/or timing can reveal whether the carried bits in each round equal zero or one, revealing some or all of the key bits" (Kocher column 5 lines 7 – 15). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence which prevents the usefulness of an attack which observes the power consumption and/or timing to determine whether the carried bits are zeroes or ones, which reveals the bits of the key.

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Leppek discloses:

A countermeasure method according to claim 3, wherein "***each of the first and second sequences is made up of the first three rounds***" (column 4 lines 10-23), wherein the encryption operators can be of any type including DES, and further, can include any number of rounds that are in each of the respective encryption operators.

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Leppek discloses:

A countermeasure method according to claim 3. Leppek does not explicitly state ***"other manipulating means consist of second means such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data."*** Kocher teaches a method of using DES to minimize information leak using smart cards and other cryptosystems, and discloses the "***complementation of the output data***" (column 6 lines 29-63, column 9 lines 5-23), where the complements are taken to prevent different sources of information leakage such as "observation of the power consumption and/or timing can reveal whether the carried bit in each round equal zero or one" (column 5 lines 8-15). This complementing of data, complements the data either at the beginning or the end, thus producing a complemented output data stream (column 9 lines 5-23). Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures.

Leppek uses a series of encryption operators with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the possibility that "observation of the power consumption and/or timing can reveal whether the carried bits in each round equal zero or one, revealing some or all of the key bits" (Kocher column 5 lines 7 – 15). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence which prevents the usefulness of an attack which observes the power consumption and/or timing to determine whether the carried bits are zeroes or ones, which reveals the bits of the key.

Claim 6 is rejected as applied above in rejecting claim 2. Furthermore, Leppek discloses:

A countermeasure method according to claim 2, wherein said "***method comprises executing a first sequence and a second sequence, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship***" (Figure 2, column 4 lines 7-52), wherein there are two different sequence of operators that can be selected randomly. Leppek does not explicitly disclose any particular encryption algorithm but states that they "need not be

any particular type of encryption algorithm" (column 4 lines 10-17). Kocher discloses the use of a modified DES encryption algorithm which consists of sixteen rounds (Figure 1), which can then incorporated in the different sequences of Leppek to produce an encrypted stream. Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures. Leppek uses a series of encryption operators with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the possibility that "observation of the power consumption and/or timing can reveal whether the carried bits in each round equal zero or one, revealing some or all of the key bits" (Kocher column 5 lines 7 – 15). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence which prevents the usefulness of an attack which observes the power consumption and/or timing to determine whether the carried bits are zeroes or ones, which reveals the bits of the key.

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Leppek discloses:

A countermeasure method according to claim 6, wherein "***each of the first and second sequences is made up of the last three rounds***" (column 4 lines 10-23), wherein the encryption operators can be of any type including DES, and further, can include any number of rounds that are in each of the respective encryption operators; and

"***wherein the other manipulating means used in the second sequence comprise second manipulating means and a third manipulating means***" (column 4 lines 10-23), wherein there can be a number of different encryption operators in each sequence, which each include different means for changing (manipulating) the data.

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Leppek discloses:

A countermeasure method according to claim 7, wherein "***said second manipulating means are used in the second sequence for the fourteenth round***" (column 4 lines 10-23), wherein the encryption operators can be of any type including DES, and further, can include any manipulation in any of the rounds, including the fourteenth round of the respective encryption operation. Leppek does not explicitly disclose ***"second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data."*** Kocher teaches a method of using DES to minimize information leak using smart cards and other cryptosystems, and discloses the "***complementation of the output data***" (column 6 lines 29-63, column 9 lines 5-23), where the complements

are taken to prevent different sources of information leakage such as "observation of the power consumption and/or timing can reveal whether the carried bit in each round equal zero or one" (column 5 lines 8-15). This complementing of data, complements the data either at the beginning or the end, thus producing a complemented output data stream (column 9 lines 5-23). Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures. Leppek uses a series of encryption operators with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the possibility that "observation of the power consumption and/or timing can reveal whether the carried bits in each round equal zero or one, revealing some or all of the key bits" (Kocher column 5 lines 7 – 15). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence which prevents the usefulness of an attack which observes the power consumption and/or timing to determine whether the carried bits are zeroes or ones, which reveals the bits of the key.

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Leppek discloses:

A countermeasure method according to claim 8, wherein "said third manipulating means are used in the second sequence for the fifteenth and the sixteenth round" (column 4 lines 10-23), wherein the encryption operators can be of any type including DES, and further, can include any manipulation in any of the rounds, including the fourteenth round of the respective encryption operation. Leppek does not explicitly disclose ***"second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data."*** Kocher teaches a method of using DES to minimize information leak using smart cards and other cryptosystems, and discloses the "***complementation of the output data***" (column 6 lines 29-63, column 9 lines 5-23), where the complements are taken to prevent different sources of information leakage such as "observation of the power consumption and/or timing can reveal whether the carried bit in each round equal zero or one" (column 5 lines 8-15). This complementing of data, complements the data either at the beginning or the end, thus producing a complemented output data stream (column 9 lines 5-23). Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures. Leppek uses a series of encryption operators with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be

conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the possibility that "observation of the power consumption and/or timing can reveal whether the carried bits in each round equal zero or one, revealing some or all of the key bits" (Kocher column 5 lines 7 – 15). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence which prevents the usefulness of an attack which observes the power consumption and/or timing to determine whether the carried bits are zeroes or ones, which reveals the bits of the key.

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Leppek discloses:

A countermeasure method according to claim 1. Leppek does not explicitly disclose "***manipulating means are constants tables***." Kocher teaches the use of tables to manipulate data (column 7 lines 15-65), wherein the tables are used as a method to minimize information leakage when using a electric component such as a smart card. The tables are filled with parameters (constants), which are preferably updated so that attackers cannot obtain the contents of the table by analysis of measurements. The Leppek and Kocher are analogous arts in that both are concerned with providing cryptosystems that take measures to make data more unpredictable than using common encryption procedures. Leppek uses a series of encryption operators

with a randomized order to obscure the encryption footprint, which exists, by using a particular encryption algorithm. Leppek stats "the encryption routines...need not be any particular type of encryption algorithm and may be conventional encryption operators, such as, PGP, DES, etc." Therefore it is obvious the modified DES presented by Kocher could be implemented in the encryption scheme of Leppek to prevent the possibility that "table lookup operations leak information about the address of the memory lookup and the value that is returned" (Kocher column 5 lines 30 – 41). Therefore it would have been obvious to one of ordinary skill in the art to combine the encryption operator of Kocher with the encryption scheme of Leppek in order to use an encryption operator in the sequence, which prevents the table lookup from leaking information about the address of the memory lookup and the returned value.

Claim 16 is rejected as applied in rejecting claim 13. Furthermore, Leppek discloses:

The electric component of claim 13. Leppek does not explicitly disclose that the countermeasure method is implemented on a "***smart card***". Kocher discloses that the technique of improving the DES against external monitoring attacks is "implementable in cryptographic smartcards" (Abstract). The encryption scheme of Leppek is used to encrypt data communications, which is analogous to the purpose of the invention of Kocher, who aims to more securely perform cryptographic processing. It is well-known in the art to use smart cards to carry and send data, because they are portable and can be associated with one user. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption scheme

of Leppek on a smart card as disclosed by Kocher to secure (encrypt) the data being processed on the smart card to prevent attackers from obtaining secret information. The implementation of the encryption scheme of Leppek on the smart card would allow information to be portable and allow the processing of that information to be secure.

6. Claims 13-15 are apparatus claims analogous to the method claims 1-10 rejected above, and therefore, are rejected following the same reasoning.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
02/10/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100